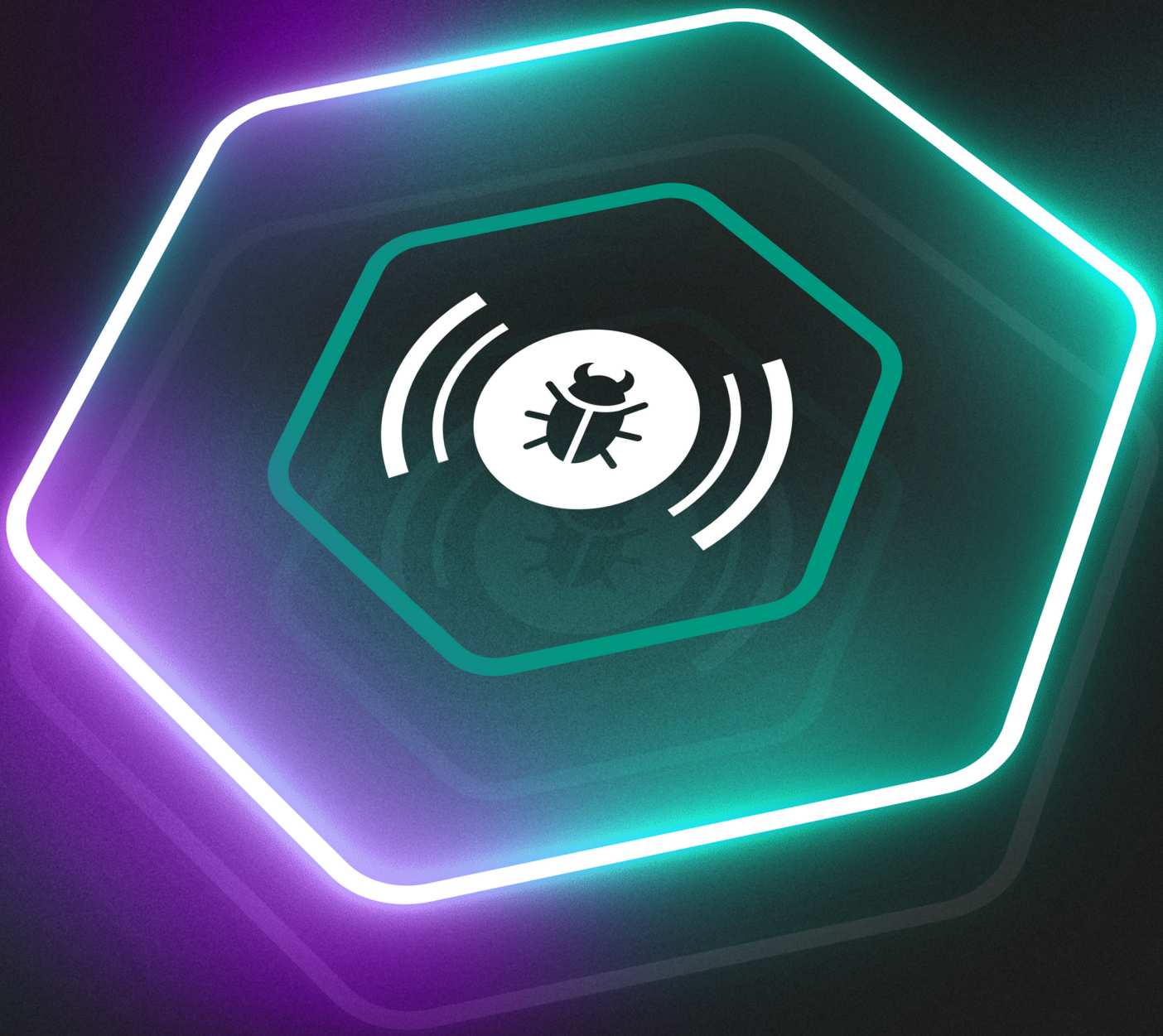


Kaspersky Threat Data Feeds

kaspersky PREPARADOS PARA EL FUTURO

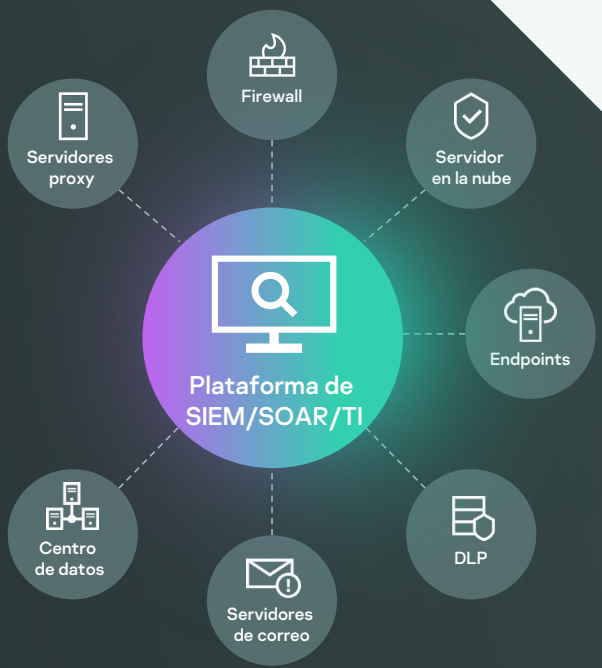
Kaspersky Threat Data Feeds

Los ciberataques ocurren diariamente. La frecuencia, la complejidad y la ofuscación de las ciberamenazas crecen de forma constante a medida que intentan comprometer sus defensas. Los adversarios utilizan complicados esquemas de ataque de intrusión, campañas, así como tácticas, técnicas y procedimientos (TTP) personalizados para interrumpir las actividades de su empresa o dañar a sus clientes. Es evidente que se necesitan nuevos métodos de protección basados en la inteligencia de amenazas.

Mediante la integración en los sistemas de seguridad existentes, como las plataformas SIEM, SOAR y de inteligencia de amenazas de las fuentes de inteligencia de amenazas actualizadas que contienen información sobre direcciones IP, URL y hashes de archivos sospechosos y peligrosos, los equipos de seguridad pueden automatizar el proceso de análisis inicial de alertas y, al mismo tiempo, ofrecer a sus especialistas en evaluación suficiente contexto para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de Respuesta a Incidentes para una mayor investigación y respuesta.

- FUENTE DE REPUTACIÓN DE IP
- FUENTE DE HASH (WIN/*nix/ MacOS/AndroidOS/iOS)
- FUENTE DE URL (maliciosas, phishing y C&C)
- FUENTE DE URL DE RAMSOMWARE
- FUENTES DE IOC DE APT
- FUENTE DE VULNERABILIDAD
- FUENTE DE DNS PASIVO (pDNS)
- FUENTE DE URL DE IoT
- FUENTE DE LISTAS DE PERMITIDOS
- FUENTE DE HASH DE ICS
- Y MÁS

Kaspersky Threat Data Feeds



Datos contextuales

Todos los registros de cada fuente de datos se mejoran con contexto útil (nombres de amenazas, marcas de tiempo, geolocalización, direcciones IP resueltas de recursos web infectados, hashes, popularidad, etc.). Los datos contextuales ayudan a revelar una "visión de conjunto", lo que mejora la validación y complementación de un uso variado de los datos. Cuando están en contexto, los datos se pueden utilizar de forma más inmediata para responder a quién, qué, dónde y cuándo, lo que permite identificar a los adversarios y ayuda a tomar decisiones rápidas y a actuar.

Aspectos destacados

Recopilación y procesamiento

Las fuentes de datos proceden de una fusión de fuentes heterogéneas de gran fiabilidad como, por ejemplo, Kaspersky Security Network y nuestros propios rastreadores web, nuestro servicio de supervisión de botnets (supervisión ininterrumpida de botnets y de sus objetivos y actividades), trampas de spam, equipos de investigación y partners.

A continuación, todos los datos agregados se inspeccionan cuidadosamente en tiempo real mediante varias técnicas de procesamiento previo, como criterios estadísticos, sandboxes, motores heurísticos, herramientas de similitud, creación de perfiles de análisis, validación de analistas y verificación de listas de permisos.

Las fuentes de datos se generan automáticamente en tiempo real, en función de las conclusiones recopiladas a nivel mundial (Kaspersky Security Network ofrece visibilidad de un gran porcentaje de todo el tráfico de Internet, con decenas de millones de usuarios finales en más de 213 países), lo que ofrece unos altos índices de detección y precisión.

Facilidad de implementación. Se combina toda la documentación complementaria, muestras, un responsable técnico de cuenta específico y el soporte técnico de Kaspersky para permitir una integración sencilla.

Los formatos de divulgación ligeros sencillos (JSON, CSV, OpenIoC, STIX) a través de HTTPS, TAXII o mecanismos de entrega específicos permiten una integración fácil de las fuentes en las soluciones de seguridad.

Las fuentes de datos repletas de falsos positivos carecen de valor, por lo que se realizan pruebas y se les aplican filtros muy exhaustivos antes de publicarlas para garantizar una distribución de datos totalmente revisados.

Cientos de expertos, entre ellos analistas de seguridad de todo el mundo, y expertos en seguridad reconocidos mundialmente de equipos GReAT y de I+D, contribuyen de forma conjunta para generar estas fuentes. Los responsables de la seguridad reciben información crucial y alertas generadas a partir de los datos de la más alta calidad, sin riesgo de que se vean desbordados por indicadores y advertencias innecesarias.

Todas las fuentes se generan y se controlan mediante una infraestructura muy tolerante a fallos, lo que garantiza una disponibilidad continua.

Ventajas

Refuerce sus soluciones de defensa de la red, como SIEM, firewalls, IPS/IDS, proxy de seguridad, soluciones DNS, protección contra APT con indicadores de compromiso (IOC) en constante actualización y contexto útil, con el fin de proporcionar información sobre ciberataques y una mayor comprensión de la intención, las capacidades y los objetivos de sus adversarios. Los principales SIEM (como HP ArcSight, IBM QRadar, Splunk, etc.) y las plataformas de TI son totalmente compatibles.

Mejore y acelere sus capacidades forenses y de respuesta automatizando el proceso de evaluación inicial y proporcionando a sus analistas de seguridad el contexto suficiente para identificar inmediatamente las alertas que se deben investigar o escalar a los equipos de respuesta de incidentes para una mayor investigación y respuesta.

Evite la exfiltración de activos y propiedad intelectual confidenciales de los equipos infectados fuera de la organización. Detecte rápidamente los activos infectados para proteger la reputación de su marca, mantener su ventaja competitiva y asegurar las oportunidades de negocio.

Como MSSP, haga crecer su empresa proporcionando inteligencia de amenazas líder del sector como servicio premium a sus clientes. Como CERT, mejore y amplíe sus capacidades de identificación y detección de ciberamenazas.

www.kaspersky.es

© 2022 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas
pertenecen a sus respectivos propietarios.